



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/626,637	07/27/2000	Deepak Gupta	JP920000150US1	9799
30449	7590	03/10/2004	EXAMINER	
SCHMEISER, OLSEN + WATTS SUITE 201 3 LEAR JET LATHAM, NY 12033			SHIN, KYUNG H	
		ART UNIT	PAPER NUMBER	
		2132		
DATE MAILED: 03/10/2004				

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/626,637	GUPTA ET AL.	
	Examiner	Art Unit Kyung Shin	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 27 July 2000.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-10 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 27 July 2000 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>7-27-00</u> .	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

- This action is responding to application papers dated 7/27/2000.
- Claims 1 – 10 are pending. Claims 1 and 6 are **independent** claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1- 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis et al. (U.S. Patent No. 6,233,565: File date is Feb. 13, 1998) in view of Perlman et al. (U.S. Patent No. 6,230,266: File date is Feb. 3, 1999).

Regarding Claims 1,6, Lewis discloses a method for enabling the use of valid authentication certificates when the private key and public key of any of the certifying authorities have expired comprising:

- a) obtaining a server certifying authority chain (SCAC) certificate by the server from the said certifying authority, (see col. 30, lines 39-41)
- b) presenting the original valid authentication certificate along with the said server certifying authority chain certificate, by the server to the browser during the SSL handshake, (see col. 14, lines 36-42, and see col. 30, lines 41-43)

c) accepting the transaction by the browser after verification of the original authentication certificate using the expired public key of the certifying authority, and verifying the said SCAC certificate using the new public key of the said certifying authority. (see col. 30, lines 43-50 : When a certificate expires, the certification authority will issue a new certificate and sign it with the old certificates matching private key. The CA will send a new certificate signed with the CA's new private key to the server. The server will validate the certificate for authenticity by first checking to ensure that the new CA certificates public key authenticates the included signature. It will then hash the keys included with the new certificate to verify that the hash value match with the old hash included with the old CA's certificate.)

Regarding Claims 4, 9, Lewis discloses a method as claimed in claim 1 wherein the certifying authority in case of client will also issue client certificates known as (CCAC) certificates, which will work the same way as (SCAC) certificates. (see col. 31, lines 30-38)

Regarding Claims 5, 10, Lewis discloses a method as claimed in claim 1 wherein during SSL handshake (see col. 14, lines 36-42) when the client presents its certificate, it will also present the CCAC certificate to the server. (see col. 31 lines 14-21)

But Lewis does not disclose when CA invalidates or withdraws its public key server certificate is obtained by each server by contacting the CA using the server's private key, verifying the request by the CA using the server's public key, generating the certificate by the CA using its new private key and forwarding to the server, and

certificate includes the authentication of the server name, the server public key, old CA public key and CA name. However, *Perlman et al.* discloses those in Authentication system and Process:

Regarding Claims 2, 7, Perlman discloses a method as claimed in claim 1 wherein the said server certifying authority chain (SCAC) certificate is obtained by each server whenever the certifying authority invalidates or withdraws its public key, by: (see col. 12, lines 9-11)

- a) contacting the certifying authority using the server's private key for authentication, (see col. 6, lines 63-6)
- b) verifying the request by the certifying authority using the server's public key, (see col. 7, lines 15-18)
- c) generating the SCAC certificate by the certifying authority using its new private key and forwarding to the said server. (see col. 7, lines 12-24)

Regarding Claims 3, 8, Perlman discloses a method as claimed in claim 2 wherein the generating of the said SCAC certificate includes the authentication of the server name and the server public key, old certifying authority public key and certifying authority name. (*Perlman*, see col. 7, lines 10-12)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inventions of *Lewis* to include when CA invalidates or withdraws its public key server certificate is obtained by each server by contacting the CA using the server's private key, verifying the request by the CA using the server's public key, generating the certificate by the CA using its new private key and forwarding

Art Unit: 2132

to the server, and certificate includes the authentication of the server name, the server public key, old CA public key and CA name as taught in *Perlman*. Therefore, one of ordinary skill in the art would have been motivated to add the invention of *Perlman* in order to issue new certification from a CA to recertify server's valid public key efficiently and securely re-establish authentication system security.

Conclusion

Prior Art

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. U.S. Patent No. 6, 367,009,322 B1 to Davis et al. discloses Extending SSL to a Multi-tier Environment using Delegation of Authentication and Authority.
- b. U.S. Patent No. 6, 668,322 B1 to Wood et al. discloses Access Management System and Method Employing Secure Credentials.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305-0711. The examiner can normally be reached on 6:30 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KHS

Kyung H Shin
Patent Examiner
Art Unit 2132

KHS
March 7, 2004

Gilberto Barron
GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100